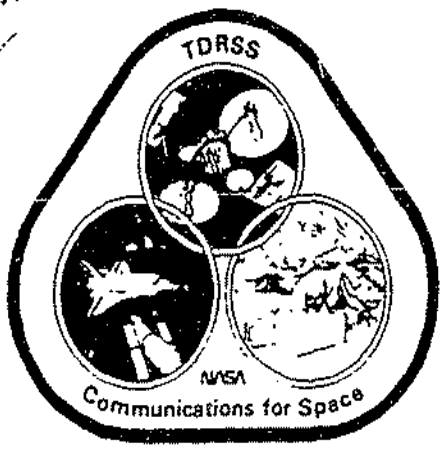
Security Classification Guide



Tracking and Data Relay Satellite System

April 15, 1982

NASA
National Aeronautics and Space Administration

TDRSS PROGRAM
SECURITY CLASSIFICATION GUIDE

APRIL 15, 1982

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
GODDARD SPACE FLIGHT CENTER
GREENBELT, MARYLAND 20771

FOREWORD

1. Purpose. This Guide provides NASA personnel, contractors, and other agencies a basis for determining the classification necessary for information and material associated with the Tracking and Data Relay Satellite System (TDRSS) and the associated ground network elements.

2. Use of the Guide. This Guide will be used as the basis for security classification determination of all documents, photographs, models, equipment, etc., pertaining to the TDRSS Program. Clarification of the guidance contained herein determined to be necessary in specific instances will be furnished by the Goddard Space Flight Center.

3. Authority. This Guide has been published under the authority of Sections 1203.202(a)(5) and 1203.412(a), NHB 1640.4, "NASA Information Security Program", dated June 1979.

4. Office of Primary Responsibility. Goddard Space Flight Center, Greenbelt, Maryland 20771.

5. Recision. This Guide supercedes previous editions of the TDRSS Security Classification Guide which should be removed from the files and destroyed.

Frank J. Simokaitis
Chairperson, NASA Information
Security Program Committee

TDRSS PROGRAM
SECURITY CLASSIFICATION GUIDE

APRIL 15, 1982

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

SECTION I

GENERAL INSTRUCTIONS

1. Introduction

This section provides definitions, classification, philosophy, and general classification instructions.

2. Definition of Terms

The following abbreviations are used in this Guide:

ADF	- Acquisition Data Facility
COMSEC	- Communications Security or, more specifically, the protection resulting from the application of cryptosecurity, transmission security, emission security, and physical security measures to communications
C	- Confidential
CSESD	- Communications Security Equipment System Document
CSS	- Control and Status System
GSFC	- Goddard Space Flight Center
NASCOM	- NASA Communications
NGT	- NASA Ground Terminal (White Sands, New Mexico)
NCC	- Network Control Center (Greenbelt, Maryland)
R	- Review
RAP	- Restricted Access Processor
S	- Secret
SCG	- Security Classification Guide
STS	- Space Transportation System
SUPIDENT	- Support Identification Code

TDRS	- A Tracking and Data Relay Satellite
TDRSS	- Tracking and Data Relay Satellite System
U	- Unclassified
Vulnerability	- Any weakness of a design, segment, system, subsystem, or communications link, the public knowledge of which, if exploited, would reduce or neutralize the effectiveness of all or part of the TDRSS
WSGT	- White Sands Ground Terminal (White Sands, New Mexico)

3. Classification Philosophy

Knowledge of the TDRSS and its operation is, for the most part, unclassified. However, the key role of TDRSS in NASA mission operations and the introduction of support for DOD missions imposes classification requirements on selected portions of the TDRSS Program. The fundamental objective for the classifications provided in this document is as follows:

a. For DOD missions, whether during STS operations or free flight, to protect information relating to:

(1) the payload mission and flight objectives;

(2) the payload mission and flight success or failure;

(3) the payload capability;

(4) the payload vulnerability; and

(5) the payload operations and schedules.

b. For the TDRSS, to protect information relating to TDRSS vulnerability and thus to inhibit interference with TDRSS support operations.

All security classification requirements can be traced to protecting this information. Data revealing the above information, by itself or in association with other available data, is classified and must be protected. The determination of the classification of data is based entirely on the potential of revealing any of the above information.

4. Classification Recommendations

a. Assistance in maintaining current, effective, logical classification criteria is solicited of all Government and industrial organizations. If classification changes are appropriate, submit documented recommendations to Security Classification Officer, Goddard Space Flight Center.

b. When the accuracy of an assigned security classification is questioned, immediately notify the Security Classification Officer, Goddard Space Flight Center. Pending review of the information, protect at the highest classification level believed to be appropriate. (Example: If the accuracy of a CONFIDENTIAL classification is questioned and the recipient believes the correct classification to be SECRET, protect the information as SECRET until the question has been resolved.)

c. In the event of a conflict between this Guide and the Security Classification guidance of related programs, inform the Security Classification Officer, Goddard Space Flight Center, for resolution.

5. Classification Currency

This Guide is in effect as of the date of issue. Revisions to this Guide will be made by distributing corrected pages to all holders for insertion in place of superseded pages; superseded pages will be destroyed. When considered appropriate, a completely revised Guide will be issued.

6. Classification/Declassification Instructions

Classification designations as specified in this Guide are identified as "S" for Secret, "C" for Confidential, and "U" for Unclassified, with a specific date for declassification as indicated for review. The declassification review date for most classified items is 1 October 2000. The duration of the classification exceeds 6 years because:

a. the continuing protection of communications security information is essential to national security; or

b. the information reveals vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to result in nullifying the effectiveness of a system, installation, or project important to the national security.

7. Dissemination Instruction

Local reproduction of this Guide is authorized.

8. Other Instructions

a. Marking and Handling. Classification designations, time limits, derivative marking procedures, and other requirements of Executive Order 12065 are to be applied to information classified pursuant to this Guide in accordance with the NHB 1620.3A, NASA Physical Security Handbook and NASA Security Procedures User Guide, and all appropriate supplements.

b. This Guide or SCG-16 will be cited as the classification authority for material generated in connection with the TDRSS Program. Information and material requiring a security classification based on requirements of other programs will be dealt with in accordance with the guidance contained in the appropriate program security classification guide.

c. SCG-16 relates to specific classification requirements which have not been included herein. SCG-16 can be obtained from the GSFC Security Office with suitable justification.

d. A compilation of unclassified items of information shall normally not be classified. Under certain circumstances, classification may be required if the combination of unclassified items of information provides insight into classified areas covered by this Classification Guide. Under this circumstance, it is the combination or compilation of information that becomes classified, not the individual item of information. Classification on this basis shall be used sparingly and shall be fully supported in written explanation which will be provided with the material so classified. Classification may not be used to limit the dissemination of information that is not classifiable within itself and on its own merits.

9. Classification of COMSEC Materials

Classification of COMSEC material and information is established in accordance with basic policy and guidance from the Director, National Security Agency. Specific classification guidance on the design, operation, capability, and characteristics of cryptographic equipment systems can be derived from COMSEC Equipment Systems Documents (CSESD's) and/or the COMSEC maintenance instructions.

SECTION II

RELEASE OF INFORMATION

1. Public Release of Information

Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination prior to submission for approval and coordination through the Goddard Space Flight Center. Contractors will be governed by the instructions contained in paragraph 13, DOD Form 254, Contract Security Classification Specifications. NASA Headquarters and field installations will follow the provisions of NASA Management Instruction 1380.4A, Release of Information to News and Information Media. Any proposed release into public domain of information pertaining to TDRSS support of a designated national security mission will be coordinated with the Office of Public Affairs, SD/PA, Space Division, Air Force Systems Command, prior to any release.

2. Release of Classified Information at Symposia, Seminars, or Technical Society Meetings

Requests for release of classified information will be submitted to the GSFC Security Office for review and approval, a minimum of 30 days prior to the proposed date of release. The request for review of the document and approval of its presentation will include the name of the individual making the presentation, the date of the presentation, title of the symposium, seminar, or technical society meetings, a statement to the effect that the paper has been reviewed for technical competency and proper security classification, and a statement that the paper does not contain information relating to an invention which has been ordered to be kept secret pursuant to the Invention Secrecy Act, Sections 181-188 of Title 35, U.S. Code.

3. Release of Classified Information to Foreign Governments

Contractors receiving requests from any agency except NASA for release of classified information to foreign governments will forward these requests to the GSFC Security Office. Attention of contractor is invited to the Department of State Traffic-In-Arms Regulation.

4. Release of Unclassified Information in Foreign Countries

Requests for release of unclassified information to a non-governmental agency or to individuals not connected with a foreign government, but located in a foreign country, will be submitted to the GSFC Security Office. This applies to material intended for release in, or by, a foreign media for presentation at an unclassified foreign symposium and for release to an individual located in a foreign country. Such material must be submitted to the GSFC Security Office in seven copies and not less than 45 days prior to the proposed date that final decision on releasability is required. The request will include the contract number, the name of the author or presenter, the name of the symposium, publication, group or individual to receive the material, and a certification that the information is unclassified, technically accurate, and suitable for public release.

5. Dissemination of Unclassified Technical Information to a Foreign Government or its Agent

Requests for dissemination of unclassified technical information to a foreign government or its designated agent will be forwarded to the GSFC Security Office.

6. Release of Classified Information to Other U.S. Agencies

Classified information and material shall be released to other federal departments or to United States industrial facilities only on a need-to-know basis and in accordance with the NHB 1620.3A, Physical Security Handbook, DOD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, DOD 5220.22-R, Industrial Security Regulation, and provided such release has been approved by the GSFC Security Office.

7. Visits by Representatives of State and Federal Government

The GSFC Security Office will be notified of any contemplated visit by members of the legislative or executive branches of the state or federal governments.* The notification will include the name(s), position, area of interest to the visitor, and the date of the proposed visit.

8. Release of COMSEC Information

No information, classified or unclassified, related to COMSEC equipments or materials may be released into the public domain without the prior approval of the Director, National Security Agency.

*To TDRSS related facilities

TDRSS PROGRAM
SECURITY CLASSIFICATION GUIDE

APRIL 15, 1982

SECTION III

PROGRAM DETAILS

	INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1.	Identification of military organizational elements using TDRSS and associated network control systems.	S Review 1 Oct 2000	Unless identified as unclassified in the Military User Project's Classification Guide.
2.	Association of TDRSS and associated network control systems with specific military satellite programs.	S Review 1 Oct 2000	Unless identified as unclassified in the Military User Project's Classification Guide.
3.	Development and production schedules.	U	
4.	Complete list of prime contractors, subcontractors or suppliers.	U	
5.	Program/title contract numbers.	U	
6.	Total projected program funding.	U	
7.	Projected funding for specific security modifications for the program.	U	
8.	Current fiscal year funding.	U	
9.	Total contract value.	U	

SECTION III

PROGRAM DETAILS (CONTINUED)

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
10. Purchase orders, shop orders, receiving reports bills of lading, shipping orders, packing instructions.	U	
11. Launch dates.	U	

SECTION IV

SYSTEM VULNERABILITY

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1. Qualitative or quantitative analyses of techniques to overcome the secure systems employed in the command and control of TDRSS and related program elements.	S Review 1 Oct 2000	
2. Qualitative or quantitative analyses or information concerning the vulnerability of the systems employed in the command and control of TDRSS and related program elements.	S Review 1 Oct 2000	
3. Summaries of outage or performance information which discloses system vulnerability.	S Review 1 Oct 2000	
4. Performance specifications or capability data which individually or collectively reveal system vulnerability.	S Review 1 Oct 2000	
5. The change in system vulnerability associated with actual or proposed modifications to hardware or software.	S Review 1 Oct 2000	

SECTION V

CRYPTOGRAPHIC HARDWARE

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1. Command authentication detail.	COMSEC-S Review 30 Oct 2010	
2. Cryptographic operational detail.	COMSEC-S Review 30 Oct 2010	
3. Mechanical detail.	U	Equipment must be completely closed and attention must not be drawn to its function when it is to be viewed externally.
a. Footprint dimensions	U	
b. Enclosure dimension	U	
c. External viewing by uncleared personnel	U	
d. Weight	U	
4. Interface specifications.	U	
5. Control signals.	U	
6. Input/output data rate.	U	
7. Equipment survivability test data.	COMSEC-C Review 30 Oct 2010	
8. Equipment tempest requirements.	COMSEC-C Review 30 Oct 2010	
9. Definitions of terms relating to tempest.	S Review 30 Oct 2010	
10. Radiation vulnerability.	COMSEC-S Review 30 Oct 2010	

SECTION V

CRYPTOGRAPHIC HARDWARE (CONTINUED)

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
11. Cryptographic function.	COMSEC-S Review 1 Oct 2000	
12. Tempest suppression measures and features.	COMSEC-S Review 1 Oct 2000	
13. Details pertaining to synchronization.	COMSEC-S Review 1 Oct 2000	
14. Number of bits in fill preamble and rate of transmission.	COMSEC-S Review 1 Oct 2000	
15. Circuit schematics and/or logic.	COMSEC-S Review 1 Oct 2000	
16. Maintenance keying variables.	COMSEC-S Review 1 Oct 2000	
17. Operational keying variables.	CRYPTO-S Review 1 Oct 2000	
18. Performance, operating or signature characteristics.	COMSEC-S Review 1 Oct 2000	
19. Lists of unclassified long titles of COMSEC equipment.	U	
20. A complete or substantially complete listing of locations holding key material.	COMSEC-C Review 1 Oct 2000	

SECTION V

CRYPTOGRAPHIC HARDWARE (CONTINUED)

ation should be released only within official channels in the t of official business. Refer to SCG-16 for further details.

	NFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
	The fact that cryptographic devices use randomizers.	U	
	The randomizer itself, or any documentation (e.g., engineering drawings) which reveal randomizer design.	COMSEC-C Review 1 Oct 2000	
	Randomizer performance data.	COMSEC-C Review 1 Oct 2000	
4.	Reliability predictions and analysis.	U	
25.	Interior viewing of equipment.	CRYPTO-S Review 30 Oct 2010	
26.	Acccess to operating or maintenance instructions and/or manuals.	COMSEC-S Review 30 Oct 2010	
27.	Information concerning key generator malfunction or failure.	COMSEC-S Review 30 Oct 2010	
28.	A listing, complete or partial, of COMSEC equipment inventory.	COMSEC-C Review 1 Oct 2000	

SECTION VI

SPACE SEGMENT SYSTEM & SUBSYSTEMS

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1. The fact that TDRSS has a secure communications capability or uses COMSEC equipment.	U	
2. Number of TDRS satellites equipped with COMSEC devices.	U	
3. Identification of specific COMSEC equipment or devices to be used by the TDRSS.	U	Prior approval of COMSEC custodian is required for any external photographs, drawings, etc., of COMSEC equipment. All unclassified external photographs, drawings, etc., of COMSEC equipment must be marked "For Official Use Only."
4. External view, photographs, artists concepts, drawings of satellite.	U	
5. Physical access to satellite or major components which would disclose system vulnerability. (See SCG-16)	S Review 1 Oct 2000	Access to cryptographic equipment containing operational keying material requires a Crypto Access Authorization at the Secret level.
6. Satellite dimensions, weight, center of gravity or moment of inertia.	U	
7. Design, specification or details of arrangement of components on space frame.	U	

SECTION VI

SPACE SEGMENT SYSTEM & SUBSYSTEMS (CONTINUED)

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
8. Subsystem or component design details or technical evaluation and test results which by themselves reveal system vulnerability.	S Review 1 Oct 2000	
9. Subsystem design requirements and general specifications which by themselves reveal system vulnerability.	S Review 1 Oct 2000	
10. Design, performance or specifications which detail secure communications components (COMSEC equipment) assemblies or subassemblies which indivually or collectively indicate communications vulnerability or operational limitations.	COMSEC-S Review 1 Oct 2000	
11. Design, performance or specification details of electrical power subsystem.	U	Unless they reveal details classified by other sections of this guide.
12. Testing for hardness, EMP, etc., and the data from such testing.	S Review 1 Oct 2000	
13. Design, performance or specification details of propulsion subsystem.	U	Unless they reveal details classified by other sections of this guide.

SECTION VI

SPACE SEGMENT SYSTEM & SUBSYSTEMS (CONTINUED)

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

	INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
14.	Design, performance or specifications of thermal control subsystem.	U	Unless they reveal details classified by other sections of this guide.
15.	Design, performance or specification details of attitude determination subsystem.	U	Unless they reveal details classified by other sections of this guide.
16.	Design, performance or specification details of attitude control subsystem.	U	Unless they reveal details classified by other sections of this guide.
17.	Design, performance or specification details of telemetry, tracking, and command subsystem.	U	Unless they reveal details classified by other sections.
18.	Launch support requirements.	U	
19.	The correlation of command bit patterns with command functions added or modified as result of security considerations.	S Review 1 Oct 2000	Software bit patterns are unclassified when not correlated with the command functions they represent.
20.	Any references to sequences of commands which might disable or permanently degrade the TDRS.	S Review 1 Oct 2000	Software bit patterns are unclassified when not correlated with the command functions they represent.

SECTION VI

SPACE SEGMENT SYSTEM & SUBSYSTEMS (CONTINUED)

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
21. Communications subsystem hardware.		
a. Receiver and components	U	
b. Transmitter and components	U	
c. Antenna and components	U	
d. Processors and components	U	
22. Power flux densities that may be present at the spacecraft.	S Review 1 Oct 2000	
23. Gain distributions of the spacecraft payload as changed by the security modifications.	S Review 1 Oct 2000	
24. Time constants of security circuitry including ALC, AGC, etc.	S Review 1 Oct 2000	
25. Individual module specifications.	U	Unless the specifications supplied compromise information covered elsewhere in this guide.
26. Characteristics of COMSEC equipment.	(Refer to Section V)	

TDRSS PROGRAM
SECURITY CLASSIFICATION GUIDE

APRIL 15, 1982

SECTION VII

WHITE SANDS GROUND TERMINAL

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1. Location of TDRSS ground station.	U	
2. Personnel manning levels, training and qualifications.	U	
3. Ground station siting criteria.	U	
4. Transmitter type, size, power.	S Review 1 Oct 2000	Only to be applied to White Sands EIRP upgrade effort.
5. Antenna gain, type, size, and patterns.	U	
6. Figure of merit (G/T).	U	
7. Number and bandwidth of carriers.	U	
8. Phase linearity.	U	
9. Reliability and maintainability parameters.	U	
10. Frequency stability.	U	
11. Radio frequency tuning range.	U	
12. COMSEC equipment nomenclature.	U	
13. TDRSS radio frequency authorizations.	U	

SECTION VII

WHITE SANDS GROUND TERMINAL (CONTINUED)

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
14. User frequency authorizations.	(Unclassified unless classified by user project office)	
15. Command and pilot uplink EIRP.	S Review 1 Oct 2000	
16. The correlation of command bit patterns with command functions added or modified as result of security considerations.	S Review 1 Oct 2000	Software bit patterns are unclassified when not correlated with the command functions they represent.
17. Any reference to sequences of commands which might disable or permanently degrade the TDRS.	S Review 1 Oct 2000	Software bit patterns are unclassified when not correlated with the command functions they represent.
18. Characteristics of COMSEC equipment.	(Refer to Section V and to SCG-16)	
19. The vulnerability of the physical access procedure to the WSGT.	S Review 1 Oct 2000	

SECTION VIII

NETWORK CONTROL CENTER

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1. Location.	U	
2. The fact that the NCC will provide support services for military communications.	U	
3. Personnel manning levels training and qualifications.	U	
4. NCC siting criteria.	U	
5. The fact that the NCC has a secure communications capability or uses COMSEC equipments.	U	
6. Identification of specific COMSEC equipments to be used by NCC.	U	
7. Design performance or specific details of the secure communications components which indicate a communication vulnerability.	S Review 1 Oct 2000	
8. Failures or anomalies of equipment implemented to assure security.	S Review 1 Oct 2000	
9. The vulnerability of any security element of the NCC.	S Review 1 Oct 2000	
10. Summaries of outage information which indicates any vulnerabilities of the security equipments.	S Review 1 Oct 2000	

SECTION VIII

NETWORK CONTROL CENTER (CONTINUED)

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
11. Any relationships between hardware and software modifications and changes to the vulnerability of NCC security equipments.	S Review 1 Oct 2000	
12. Design details or technical evaluation and test results which indicates any vulnerabilities of the security elements of the NCC.	S Review 1 Oct 2000	
13. Analyses which indicate any vulnerabilities of the security elements.	S Review 1 Oct 2000	
14. Penetration test results which indicates any vulnerabilities of security elements.	S Review 1 Oct 2000	
15. Information relative to the RAP data base which indicates a method for penetrating or disabling the RAP.	S Review 1 Oct 2000	
16. The fact that the RAP is operating or has operated in a failed or degraded mode.	S Review 1 Oct 2000	
17. Operating procedures that alter the vulnerability of security elements.	S Review 1 Oct 2000	
18. Characteristics of COMSEC equipment.	(Refer to Section V and to SCG-16)	

TDRSS PROGRAM
SECURITY CLASSIFICATION GUIDE

APRIL 15, 1982

SECTION IX

NASA GROUND TERMINAL

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1. Location of the NASA Ground Terminal.	U	
2. The fact that the NGT will provide support services for military communications.	U	
3. Vulnerability of the physical access to the NGT.	S Review 1 Oct 2000	
4. Personnel manning levels, training, and qualification.	U	
5. NGT siting criteria.	U	
6. The fact that the NGT has a secure communications capability or uses COMSEC equipment.	U	
7. Identification of specific COMSEC equipment to be used by the NGT.	U	
8. Design performance or specification details of secure communications components which indicate communication vulnerability.	S Review 1 Oct 2000	
9. Summaries of outage information which might indicate system vulnerabilities.	S Review 1 Oct 2000	
10. Characteristics of COMSEC equipment.	(Refer to Section V and to SCG-16)	

SECTION X

NASCOM FACILITIES

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1. Location of CSS.	U	
2. The fact that the CSS will schedule NASCOM for DOD support.	U	
3. Vulnerability of the physical access to the CSS.	S Review 1 Oct 2000	
4. Personnel manning levels, training, and qualifications.	U	
5. The fact that the CSS has a secure communications interface.	U	
6. Design, performance, or specific details of the secure communications components which indicate a communication vulnerability.	S Review 1 Oct 2000	
7. Failure or anomalies of the security equipment.	S Review 1 Oct 2000	
8. The vulnerability of any security element of the NASCOM.	S Review 1 Oct 2000	
9. Summaries of outages information which might indicate any vulnerability of the security equipment.	S Review 1 Oct 2000	

SECTION X

NASCOM FACILITIES (CONTINUED)

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
10. Any relationships between hardware and software modifications and changes to the vulnerability of NASCOM security equipment.	S Review 1 Oct 2000	
11. Design details or technical evaluation and test results which indicates any vulnerability of NASCOM security equipment.	S Review 1 Oct 2000	
12. Analyses which indicate any vulnerability of NASCOM security elements.	S Review 1 Oct 2000	
13. Penetration test results which indicate any vulnerability of security elements.	S Review 1 Oct 2000	
14. Information relative to the CSS data base which indicates a method for penetrating or disabling the CSS.	S Review 1 Oct 2000	

TDRSS PROGRAM
SECURITY CLASSIFICATION GUIDE

APRIL 15, 1982

SECTION XI

TDRS OPERATIONS DATA

Information should be released only with official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1. Frequency bands.	U	
2. Data rates.	U	
3. Exact system operating frequencies.	U	
4. Telemetry and tracking data.	U	
5. Encrypted telemetry.	U	
6. Housekeeping and status data.	U	
7. Testing or simulation data.	U	
8. Testing, simulation, housekeeping and status data of cryptographic equipment.	(Refer to SCG-15 and Section V of this guide)	
9. Operations, logistics or maintenance manuals.	U	Unless revealing details classified by other sections of the guide.
10. Failure/anomalies of COMSEC equipment.	COMSEC-S Review 1 Oct 2000	
11. Operations, logistics or maintenance manuals for COMSEC equipment.	(Refer to SCG-16 and Section V of this guide)	

SECTION XI

TDRSS OPERATIONS DATA (CONTINUED)

Information should be released only with official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
12. In the event of a launch failure resulting in impact on either land or sea outside a designated landing area, no information will be released concerning the location of the recovery area. This is to prevent unauthorized access to classified equipment/ information. If the equipment cannot be secured and search is terminated, the exact location of the recovery area shall be classified.	COMSEC-S Review 1 Oct 2000	
13. RFI test data including specific RFI surveys and RFI data acquired during normal operation which is specifically isolated and recorded.	S Review 1 Oct 2000	

SECTION XII

DOD USER OPERATIONS DATA

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details. Some, but not all, of the requirements of this section are derived from the STS Classification Guide. For specific classification requirements for the STS program refer to the AFSD STS Security Classification Guide.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
1. Planning data for DOD STS and Free Flyer missions.	S Review 31 Oct 2009	Unless declassified by DOD user project.
2. DOD STS acquisition, and ephmeris data.	S Review 1 Dec 1998	Secret until 2 hours prior to event, unclassified thereafter.
3. DOD Free Flyer acquisition, tracking, and ephemeris.	S Review 31 Oct 2009	Unless declassified by DOD user project.
4. Encrypted user data.	U	
5. DOD STS real-time tracking data.	U	
6. DOD user schedules.	S Review 31 Oct 2009	Unless declassified by DOD Project.
7. TDRSS real-time operational status in support of DOD Free Flyer or DOD payload.	S Review 31 Oct 2009	Confidential if ephemeris or payload signature information is not revealed.
8. TDRSS historical operational status in support of DOD Free Flyer or DOD payload.	C Review 1 Oct 2009	DOD STS historical data is unclassified if not payload unique.

SECTION XII

DOD USER OPERATIONS DATA (CONTINUED)

Information should be released only within official channels in the conduct of official business. Refer to SCG-16 for further details.

INFORMATION REVEALING	CLASSIFICATION DOWNGRADE/ DECLASSIFY	REMARKS
9. Information that would identify a DOD Free Flyer mission profile, DOD payload performance on-orbit, DOD payload-to-orbiter unique data interfaces, DOD payload or Free Flyer physical and system characteristics or signature.	S Review 1 Oct 2009	
10. Launch window length and constraints associated with a specific DOD payload or DOD Free Flyer.	S Review 1 Oct 2009	
11. DOD mission contingency failure reports or inputs to reports.	S Review 31 Oct 2009	Unless declassified by DOD project.
12. Information that would reveal the association of a specific DOD payload or DOD Free Flyer project with its assigned supident.	S Review 31 Oct 2009	Unless declassified by DOD project.

TDRSS PROGRAM APRIL 15, 1982
SECURITY CLASSIFICATION GUIDE

SECTION XIII

DISTRIBUTION

Director of Freedom of Information and Security Review
Office of Assistant Secretary of Defense (Public Affairs)
Washington, DC 20301

Director of Information Security
Office of the Deputy Under Secretary of Defense (Policy)
Washington, DC 20301

National Security Agency
Ft. Meade, MD 20755

Space Communications Company
1300 Quince Orchard Blvd.
Gaithersburg, MD 20878
Attention: Mr. A. Garman

TRW
Defense and Space Systems Group
One Space Park
Redondo Beach, CA 90278
Attention: J. Wellens

Harris Government Communications Systems
P.O. Box 37
Melbourne, FL 32901

Headquarters, Space Division (AFSC)
Los Angeles Air Force Station
P.O. Box 92960, Worldway Postal Center
Los Angeles, CA 90009
Attention: YOS, SP, YVA, YOOX

NASA Headquarters
Code T
Washington, DC 20546